Введение

Стремительное развитие технологий виртуализации и создание сред облачных вычислений формирует новые источники угроз, которые необходимо учитывать при обеспечении кибербезопасности современных компьютерных систем и сервисов. При этом динамический характер процессов информационного взаимодействия существенно затрудняет возможности оперативной оценки рисков нарушения конфиденциальности, целостности и доступности программных и инфраструктурных ресурсов, предоставляемых в режиме удаленного доступа. Традиционные средства обеспечения информационной безопасности (*средства разграничения доступа, межсетевые экраны, системы обнаружения вторжений и т.п.)* контролируют только те информационные потоки, которые проходят по каналам, предназначенным для их передачи, поэтому- угрозы, реализуемые посредством скрытых каналов передачи информации, с их помощью не могут быть блокированы. В этих условиях важное значение приобретают технологии защиты от угроз, которые формируются с использованием скрытых каналов информационного воздействия или внутри периметра безопасности корпоративной компьютерной сети. Защита от таких деструктивных воздействий должна осуществляться на уровне процессов управления системными вызовами или контроля недекларированных возможностей (НДВ) прикладного программного обеспечения (ПО), что требует создания новых моделей и методов противодействия попыткам внешних и внутренних пользователей изменить состояние защищенности информационных ресурсов среды облачных вычислений.

Актуальность решения этой важной научно-технической задачи отмечается многими российскими и зарубежными учѐными, в том числе В.А. Курбатовым. П.Д. Зегждой. А.А.Грушо, В.Ю. Скибой, Н А. Гайдамакиным. А.А. Гладких. В.С. Заборовским. С. Воглом. Р. Сэйлером. Ф. Мортинелли. Дж. Рутковской и др. В работах перечисленных авторов